REPORT DOCUM	ENTATION PAGE	AFRL-S	R-BL-TR-01-	
Public reporting burden for this collection of information is est gathering and maintaining the data needed, and completing an	nd reviewing the collection of i	esponse, includinformation. Ser	0088	ces, this
collection of information, including suggestions for reducing the Davis Highway, Suite 1204, Arlington, VA 22202-4302, and	nis burden, to Washington Head to the Office of Management at	nu Budget, Fapt		rson
1. AGENCY USE ONLY (Leave blank) 2. RI	PORT DATE	3. REPORT ITE A		
A STATE OF THE STA		01 M	1ay 1997 - 31 Dec 1998 5. FUNDING NUMBERS	
4. TITLE AND SUBTITLE Turbo Decoding of High performance Error	or-Correcting Codes v	via Relief Propagation	F49620-97-1-0313	
Turbo becoming of their performance and	n-concoming cours .	In Donor Kropupania	1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
6. AUTHOR(S) Robert McEliece				
Notes Medical				
7. PERFORMING ORGANIZATION NAME(S) A	ND ADDRESS(ES)		8. PERFORMING ORGANIZATI	ON
Department of Electrical Engineering			REPORT NUMBER	
MS 136-93				
California Institute of Technology				
Pasadena, CA 91125				
9. SPONSORING/MONITORING AGENCY NAM AFOSR	IE(S) AND ADDRESS(E	S)	10. SPONSORING/MONITORIN AGENCY REPORT NUMBER	
801 North Randolph Street, Room 732			E40600 07 1 0010	
Arlington, VA 22203-1977			F49620-97-1-0313	
11. SUPPLEMENTARY NOTES				
11. SUFFLEWENTANT NOTES			•	
		AIR FORCE OFFICE OF S	CIENTIFIC RESEARCH (AFOSR)	
12a. DISTRIBUTION AVAILABILITY STATEMEN		NOTICE OF TRANSMITTA	DAID: PHISTEURNICAL REPORT	
Approved for Public Release. Distribution	ınlımıtea.		D IS APPROVED FOR PUBLIC RELEASE	
		LAW AFR 190-12, DISTRI	BUTION IS UNLIMITED.	
13. ABSTRACT (Maximum 200 words)		1 let en besité f	C - 11tional andor	
We studied AWGN coding theorems for en interconnected with random interleavers. V				
classical turbo codes and the serial concater				
the behavior of the ensemble (maximum-lik				
We proved this conjecture for a simple clas				
code and th inner code is rate 1 convolution				
accumulate) codes. This was the first rigor				
	_			
	÷ .			
, •				
5				
	200402	20 013		
	ZUU IU Z	LIU UIJ		
14. SUBJECT TERMS		2.244.5	15. NUMBER OF PAG	ES
14. 665616. 12		·	1	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION 18. SECURI OF REPORT OF THIS	TY CLASSIFICATION S PAGE	19. SECURITY CLASSIFI OF ABSTRACT	CATION 20. LIMITATION OF A	3STRAC1

FINAL TECHNICAL REPORT on AFOSR grant no. F49620-97-0313:

"Turbo Decoding of High performance Error-Correcting Codes via Belief Propagation"

PRINCIPAL INVESTIGATORS:

Robert J. McEliece Department of Electrical Engineering MS 136-93 California Institute of Technology Pasadena, CA 91125

Padhraic Smyth
Department of Information and Computer Science
University of California
Irvine, CA

OBJECTIVES: No change from those stated in the original proposal.

STATUS OF EFFORT: The work went extremely well at both institutions. We had frequent joint meetings (approx. 1 per month) in which each group informed the other about its progress. Technical details follow.

ACCOMPLISHMENTS/NEW FINDINGS:

***At Caltech:

We studied AWGN coding theorems for ensembles of coding systems which are built from fixed convolutional codes interconnected with random interleavers. We call these systems "turbo-like" codes and they include as special cases both the classical turbo codes and the serial concatenation of interleaved convolutional codes. We offered a general conjecture about the behavior of the ensemble (maximum-likelihood decoder) word error probability as the word length approaches infinity. We proved this conjecture for a simple class of rate 1/q serially concatenated codes where the outer code is a q-fold repetition code and the inner code is a rate 1 convolutional code with transfer function 1/(1+D). We call these codes "RA" (repeat and accumulate) codes. This was the first rigorous proof of a coding theorem for turbo-like codes.

These results show that the performance of RA codes with maximum-likelihood decoding is very good. However, the complexity of ML decoding of RA codes, like that of all turbo-like codes, is prohibitively large. But an important feature of turbo-like codes is the availability of a simple iterative, message passing decoding algorithm that approximates ML decoding. We wrote a computer program to implement this "turbo-like" decoding for RA codes with q=3 (rate 1/3) and q=4 (rate 1/4), and the results were remarkably good. For example, with an information block length of 16384, the q=4 RA code achieves a decoded word error probability of about 10^{-5} at E_b/N_0 = 0.5 dB with 20 decoding iterations.

This work demonstrated that there is a much less complex way to achieve near Shannon limit performance than was previously suspected.